Avira Managed Email Security

AMES

HowTo

AVIRA

Table of content

1. Introduction 4

2. Getting started 4
   2.1. AMES access 4
   2.2. Licensing AMES 5
      2.2.1 Trial license 5
      2.2.2 Commercial License 6
   2.3. Logging in to AMES 7

3. Configuring the domain 8
   3.1. The Domain status assistant 8
   3.2. Configuring the DNS server 9
   3.3. Configuring the firewall 10
   3.4. Scanning outgoing Emails 10

4. User settings for AMES domains 10
   4.1. General settings 10
   4.2. Setting the user services 11
   4.3. The user account of a domain 11
   4.4. Adding a new user 12
   4.5. Adding multiple users 13
   4.6. Adding a user alias 14
   4.7. Resetting user passwords 15

5. Quarantine management 15
   5.1. Handling intercepted spam or viruses 16
   5.2. Adjusting the Spam Filter 17
   5.3. Adjusting the Content Filter 18
   5.4. Setting up virus and spam notifications 19

5.5. Managing the quarantine via the Email account 20
5.6. Managing the quarantine via the AMES account 21
5.6.1 Virus quarantine 22
5.6.2 Spam quarantine 22
5.6.3 Content Filter quarantine 23

6. User management 24
6.1. Advanced mode 24

7. Statistics 26

8. Support 27

1. Introduction

Avira **M**anaged **E**mail **S**ecurity (AMES) is an „in the cloud“ based service, which increases the security of Email traffic by stopping potential viruses and spam messages even before they reach the company IT network.

This optimal security is made possible while the Emails are first of all routed to the Avira AMES server cluster. AMES scans there all messages and forwards immediately all malware-free Emails to the Email server of the customer. Infected Emails and spam messages will be isolated in a quarantine area so that they cannot cause any harm at the customers company.

For scanning and intercepting spam messages AMES is using an extremely effective combination of technologies. Since spammers and virus makers become more skilled every day, we constantly test and implement new methods to keep our lead position in Email scanning, and you enjoy the benefits of this without any extra effort.

The data processing in an „in-the-cloud“ service is performed via the Internet, thereby the software, resources and information are located on servers placed elsewhere („in the cloud“).

Especially because AMES is an „in the cloud“ solution and is physically located in the infrastructure of the Avira data center, it eliminates the hosting, administration and the complete support on the customer‘s side. Companies do not need to invest in any hardware or software and will be freed at the same time from the entire flood of spam.

2. Getting started

2.1. AMES access

Because AMES is a cloud-based service it is possible to access the AMES user interface from any location where Internet access is provided.
The login to the AMES interface can take place either the Avira website, or via the direct AMES link: https://ames.avira.com.

Currently, the AMES interface is available in the following languages:

- English
- German
- French
- Spanish
- Dutch

AMES saves your language preference in a cookie or tries to match your browser's language. In case of an unsupported language, the AMES interface opens in English.

2.2. Licensing AMES

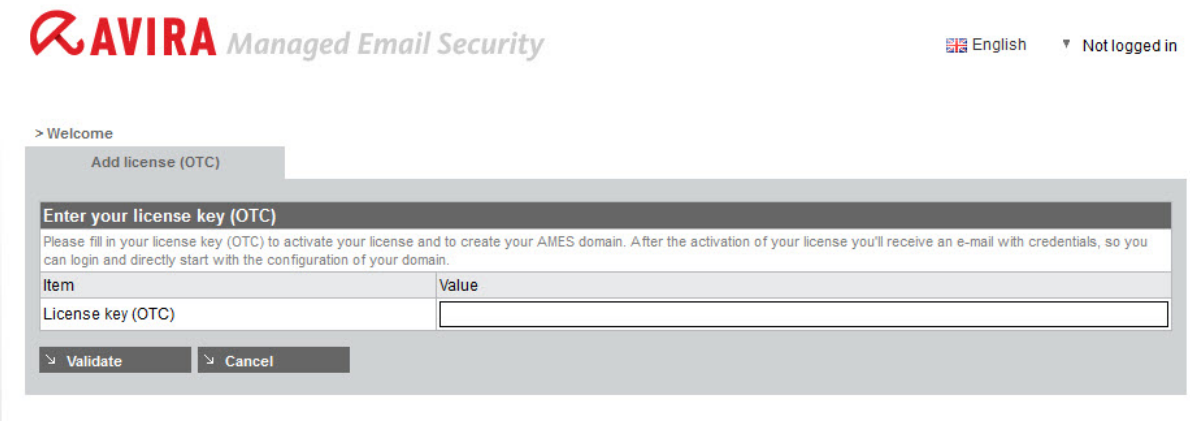
Due to the flexible Avira licensing program you can buy a license quite individually according to your needs. The licensing is based on the amount of users and is available from five or more users. The user licenses are not restricted to one customer domain. Per user can be assigned any number of Email aliases.

- One license covers your entire Email infrastructure
- License periods: 12, 24 or 36 months
- Automatic license extensions
- Flexibility to purchase additional services à la carte

2.2.1 Trial license

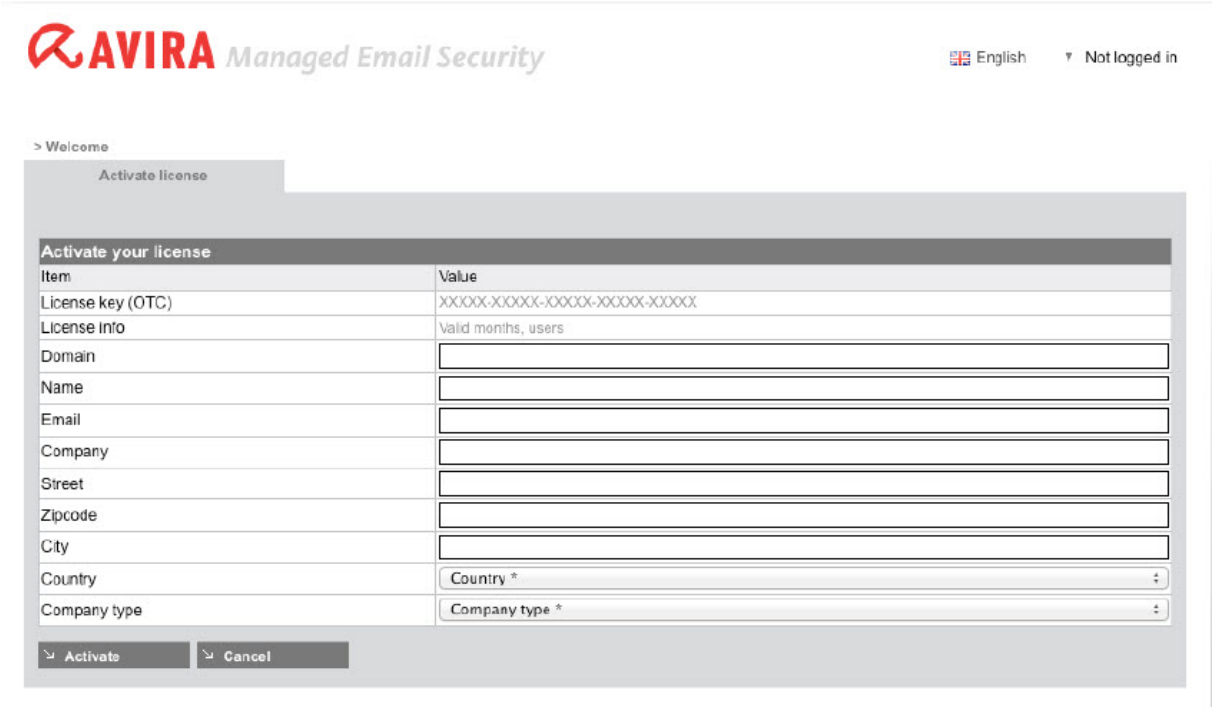
As an end user, you can request an evaluation license on the Avira website. Afterwards you will receive an OTC Key (One-Time-Code) via Email.

Activate your license by entering the OTC Key in the AMES user interface.


AVIRA Managed Email Security
English
Not logged in
> Welcome
Add license (OTC)
Enter your license key (OTC)
Please fill in your license key (OTC) to activate your license and to create your AMES domain. After the activation of your license you'll receive an e-mail with credentials, so you can login and directly start with the configuration of your domain.
Item
Value
License key (OTC)
Validate
Cancel

Note
Please note that you do not need to login to activate your license.

Once your OTC key is validated, you will be prompted to fill out a form with all the relevant information to create an AMES domain.



After the license is activated you will receive an Email with the login credentials, thereby you can log in and configure the domain.

Note
The credentials for AMES will be sent to the Email address specified in the form.

2.2.2 Commercial License

For activating a commercial license you can follow the same process as for a trial license. The only difference is that for a commercial license, the OTC key will be created by an Avira representative, or by one of its partners or distributors.

For your convenience, the sales representative will already have entered all known information, leaving only a few empty boxes for you to fill out.

If you purchase a license through your *Avira partner*, you need to select the required number of users. This corresponds to the number of employees in the company who will be using the filtered AMES Emails.

AMES gives you the opportunity to use these users across multiple domains, to create aliases for them and much more.

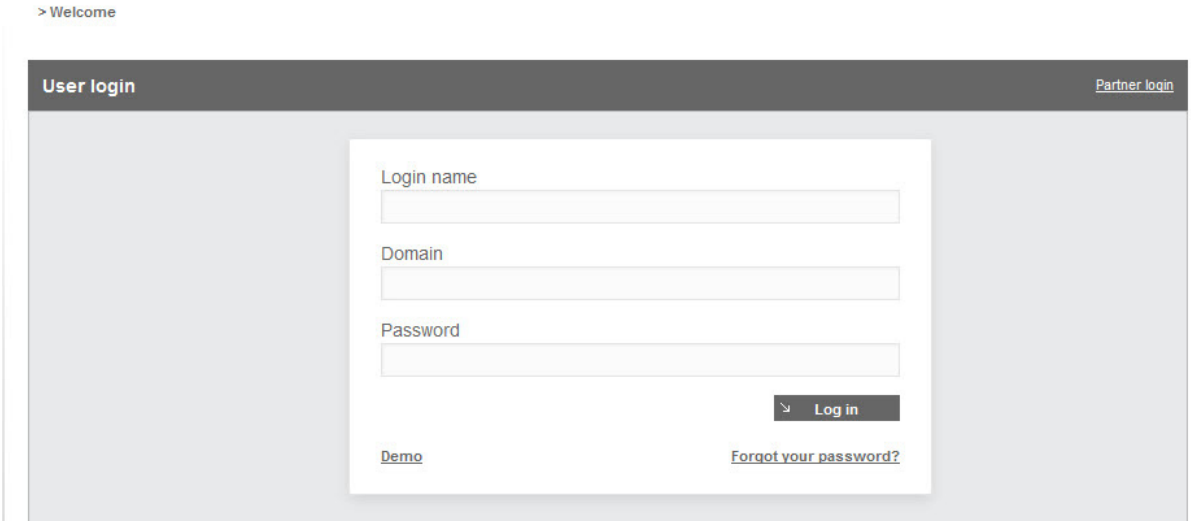
Note
It is important to adjust the license to the current number of users.

After activating the license, you will receive an Email with the login credentials which you will need later on for your login and for your domain configuration.

2.3. Logging into AMES

Once the license was successfully activated, you will receive an order confirmation Email with the necessary AMES credentials and details of the *DNS MX records* as well as the *firewall settings*.

Log on with the received *user name*, *domain*, and *password*, into the AMES user interface.



After you have logged in, you need to read and accept the *AMES SLA agreement* in order to continue.

3. Configuring the domain

If you purchased your license via the *Avira partners*, your new AMES domain has already been set.
For each new domain, one generic user is created and the mail delivery is set to the currently used mail server. This means, you can start using AMES without any further configuration and the Email flow to this user will not be interrupted.

In case you do not have any Avira partner, it is worth looking into the Avira Partner search on our website.

If you still need to perform the configuration of the domain by yourself, follow the procedure described by us.

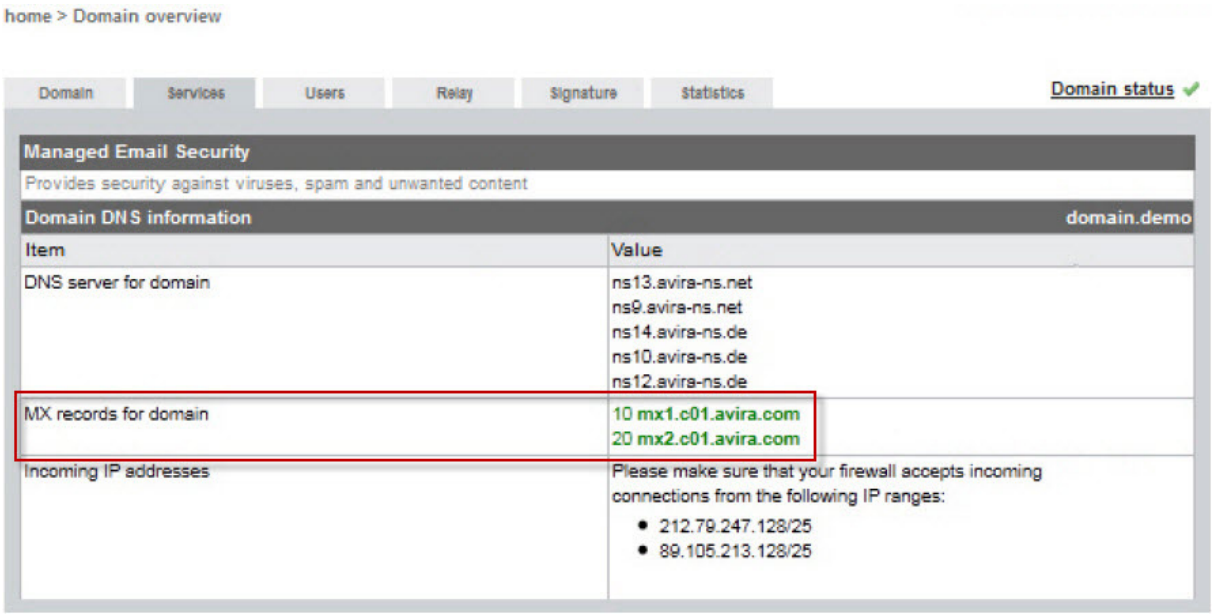
3.1. The Domain status assistant

The Domain status link opens the 5-step domain activation assistant, which shows the status of each step and eventually displays instructions to complete them:

- Domain validation
- Mail server delivery
- DNS settings
- Firewall settings
- User configuration

3.2. Configuring the DNS server

After logging into AMES, click in the domain overview on the tab *Services*.
To activate the scanning and filtering of incoming Emails, you have to adjust the MX-settings in the DNS server for the domain of your provider. Only then will the „clean“ Emails be forwarded to your mail server. The correct records are in the order confirmation that you received via Email.



The MX records should look like this:

10 mx1.c01.avira.com
20 mx2.c01.avira.com

Note
Make sure there is no MX-record with a priority below 10; otherwise Emails from your organization will not be scanned and filtered by AMES.

After directing the MX records to the Avira AMES cluster, the managed service is active and will scan and filter the incoming Emails. The filtered and scanned Emails will be delivered to the regular mailbox.

Note
Depending on the Time-To-Live (TTL) settings of your MX records, it might take up to 24 hours before DNS changes become active. During this period it may happen that Emails will be delivered to your Email server over the old routing without any AMES Filtering.

3.3. Configuring the firewall

After DNS changes are complete and propagated correctly, make sure the receiving mail server accepts only Emails coming from the AMES server cluster mentioned in the order confirmation Email. This can be done through settings in the firewall or mail server itself.

3.4. Scanning outgoing Emails

By default, AMES scans only the incoming Emails.

> **Note**
> The relay service for outgoing Emails is not part of the default mail filtering service and is therefore initially deactivated.

If you want AMES to scan your outgoing Emails for viruses, please contact your Avira partner, to activate the relay feature for your domain. With enabled relay service, the domain's administrators will see the amount of filtered outgoing messages.

4. User settings for AMES domains

4.1. General settings

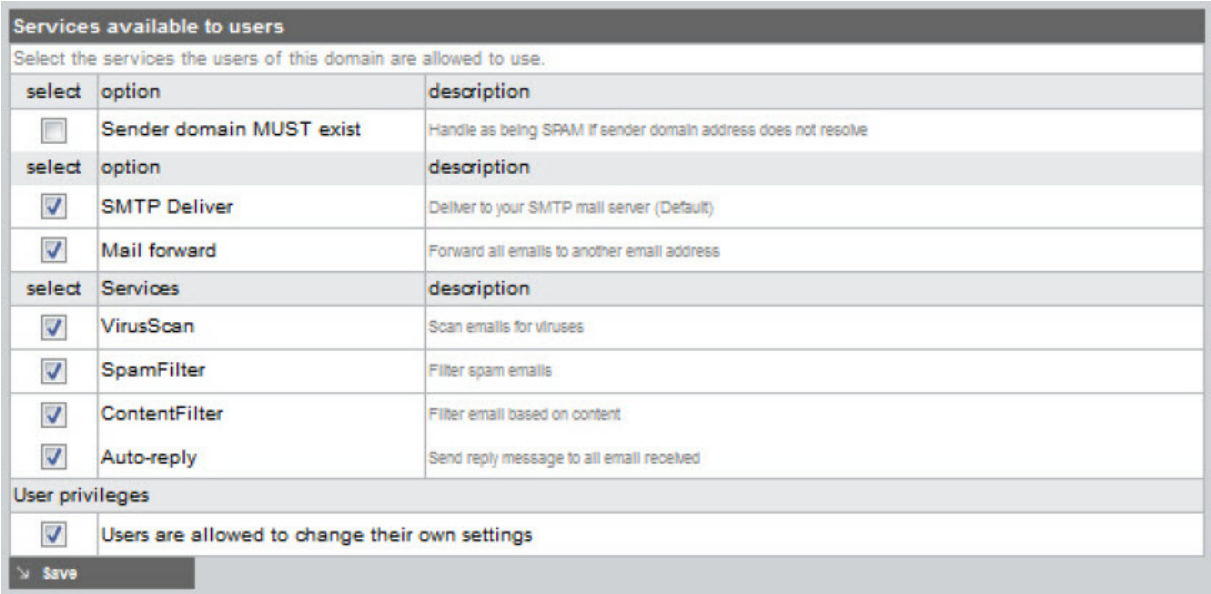
Via the link *Domain status* you can open the wizard for the domain activation.
Click in the *Domain overview* on the tab *Domain* and check the general settings of the new domain.

If necessary you can complete the configuration, such as:

- Email domain administrator
- Default incoming SMTP server(s) which will apply to the new users you create
- Apply settings for all domain users Blocked recipients
- Type of quarantine release

4.2. Setting the user services

In the *Domain overview*, click the *Services* tab. Under Services available to users, you can enable or disable certain options for all the end-users of the selected domain.



4.3. The user account of a domain

When AMES is configured for your domain, the users you provide have to operate properly. If an Email is sent to a user who is not registered in AMES, the system will refuse to forward the Email and will send it back to the sender.

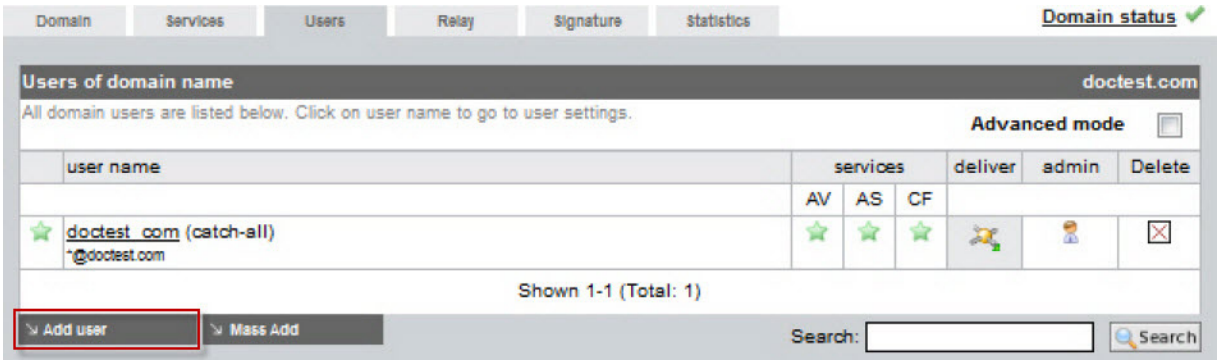
AMES has by default one *catch-all users* alias. This *catch-all user* is advantageous because it delivers all received Emails, e.g. to an *info@customer* Email address.

However, it is recommended, that each user has his own AMES account.

Note
Creating a AMES account for each user, allows the domain synchronization (LDAP / CSV).

4.4. Adding a new user

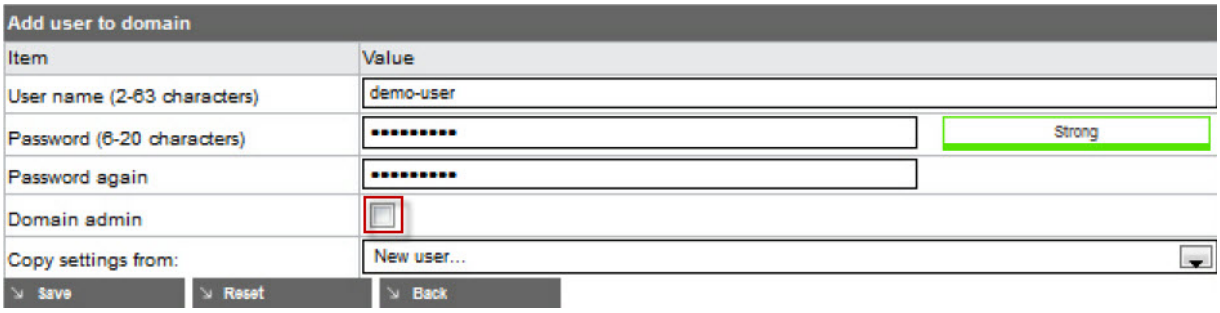
To add a new user manually, go to the *Domain overview* and click the *Users* tab.



Choose a username and password for your new user.
The password must be at least 6 characters. While typing the password strength is displayed.

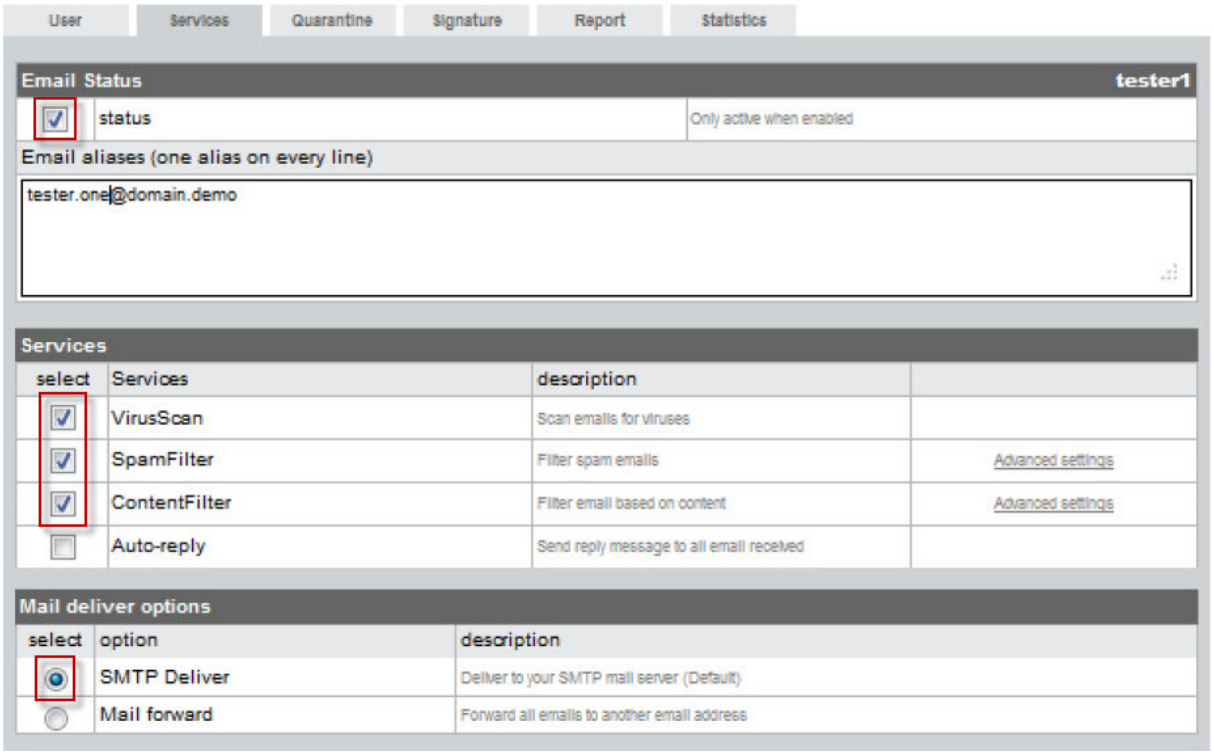
> **Note**
> Each User name is considered to be the primary Email address of that user; any other Email address of that specific user is considered an alias.

If you would like this user to be able to manage the domain's settings, than enable the *Domain admin* option.



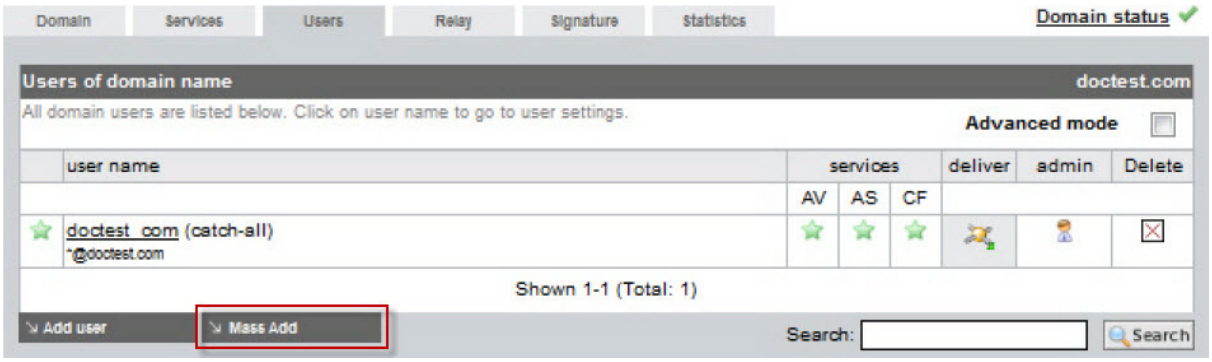
With a click on **Save** the new user will be created, but the user is disabled by default. This allows you to check once again the settings before they take effect.

To enable the user, click its name in the *User* tab and activate afterwards the *status* option, the available *Services* and the *Mail deliver options* in the *Services* tab.



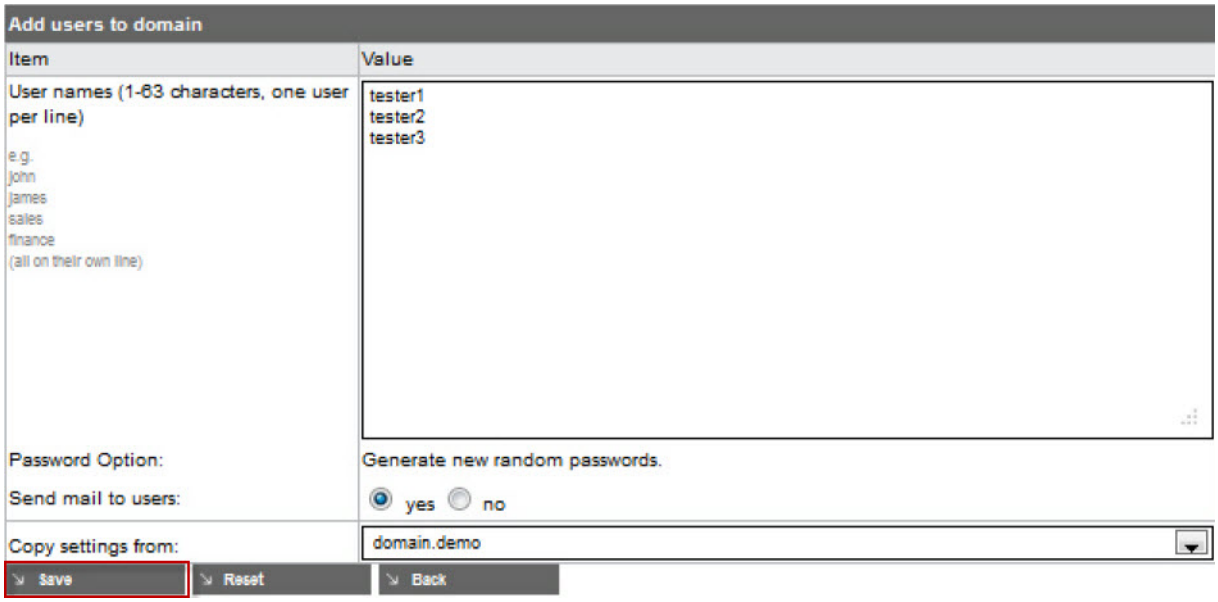
4.5. Adding multiple users

To add multiple users at once, go to the *Domain overview*, click the *Users* tab and press **Mass Add**.



Insert the names of the new users, one per line, in the *User names* area. You can apply the settings from an existing user, by selecting it from the drop-down list *Copy settings from*.The **Mass Add** feature generates random passwords and sends them by Email to the users, if the option *Send mail to users* is set to *yes*.

After saving the settings a message is displayed, with the list of users and passwords added to the domain. The AMES mail admin can store these passwords in case the user accidentally deletes the Email with the password.



Note
It is recommended to create a template called *User*, wherein all settings are preconfigured. Therefore the adding of further users is considerably simplified by copying the settings from the template *User.* Thus no further adjustments need to be made for the new added user.

4.6. Adding a user alias

User aliases can be used to assign multiple Email addresses to one user. To create an alias, select an user and go to the tab *Services*.

Add one or more Email addresses in the Email aliases field (e.g. tester.one@domain.demo). Insert each of them on a new line, not separated by other characters.

Note
If you'd like to use a *catch-all address*, use the * placeholder **@domain.demo*.
The disadvantage of an *catch-all address* is that all Email addresses are accepted and thereby the domain will be very vulnerable to spam and viruses.

Note
The ones from AMES automatically generated *catch-all forwardings* are making use of an „advanced greylisting". This technique bounces Emails from unknown senders the first time, and will accept only the second or later attempt.
Because spam servers will not try to resend Emails, greylisting significantly reduces the amount of Emails that must be filtered and scanned.

4.7. Resetting user passwords

Domain administrators and Avira partners can reset the passwords of all users of a domain, by generating random passwords.

To reset all user passwords within a domain, go to the *Domain overview*, click the *Services* tab and scroll down to the *Password reset* section.
To create a new password, click **Reset password**. Afterwards a list of all generated passwords will be displayed.

If you did not enable the option *Send mail to users*, make sure you save this list and send the credentials to each of the users.

If the option *Send mail to users* is enabled the new users credentials are automatically sent to the affected users via Email.

5. Quarantine management

AMES comprises a variety of Email filtering and analysis tools. You can configure your AMES account to remove infected Emails immediately, to send them to quarantine or just to place a tag in their subject.

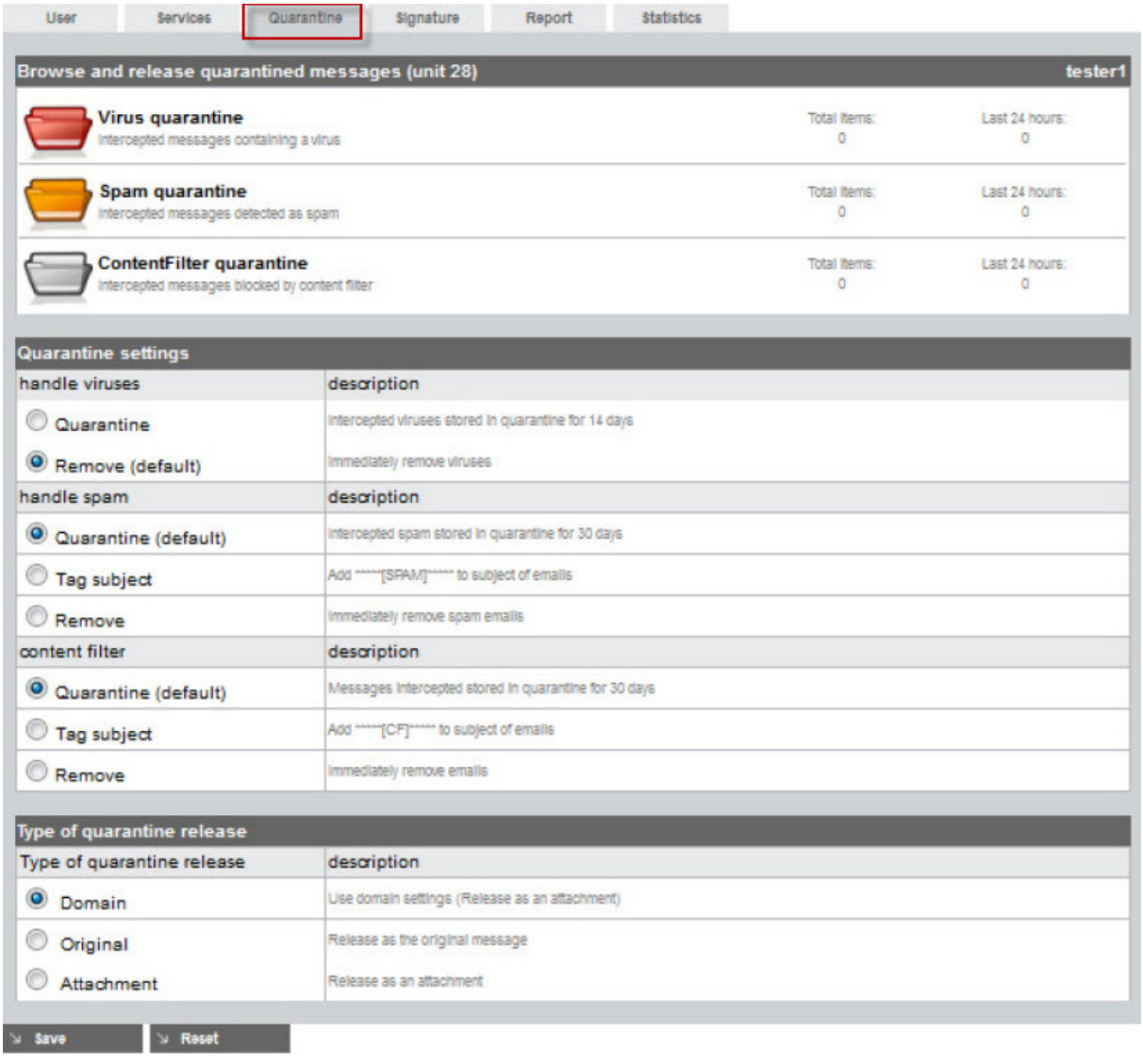
Furthermore, you can modify the heuristic level of the spam control, define advanced spam rules and content filtering rules.

Note
A domain administrator can in accordance with their corporate security policy to configure the filter, quarantines and reports and disable these options for the end users.

5.1. Handling intercepted spam or viruses

If during the filtering process AMES intercepts infected Emails, they are moved by default to quarantine. However, there is also the possibility to mark these Emails before delivering them to the inbox, or to delete them immediately.

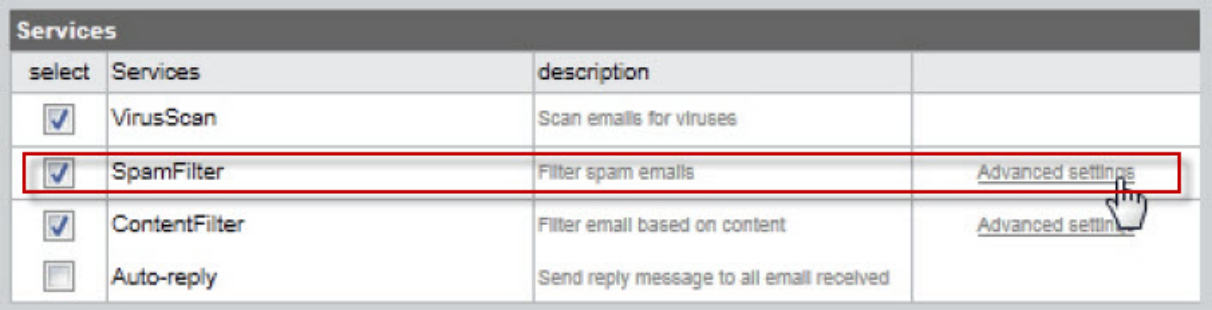
To change the settings, select the corresponding user for whom you would like to configure the spam and virus handling and click the *Quarantine* tab.



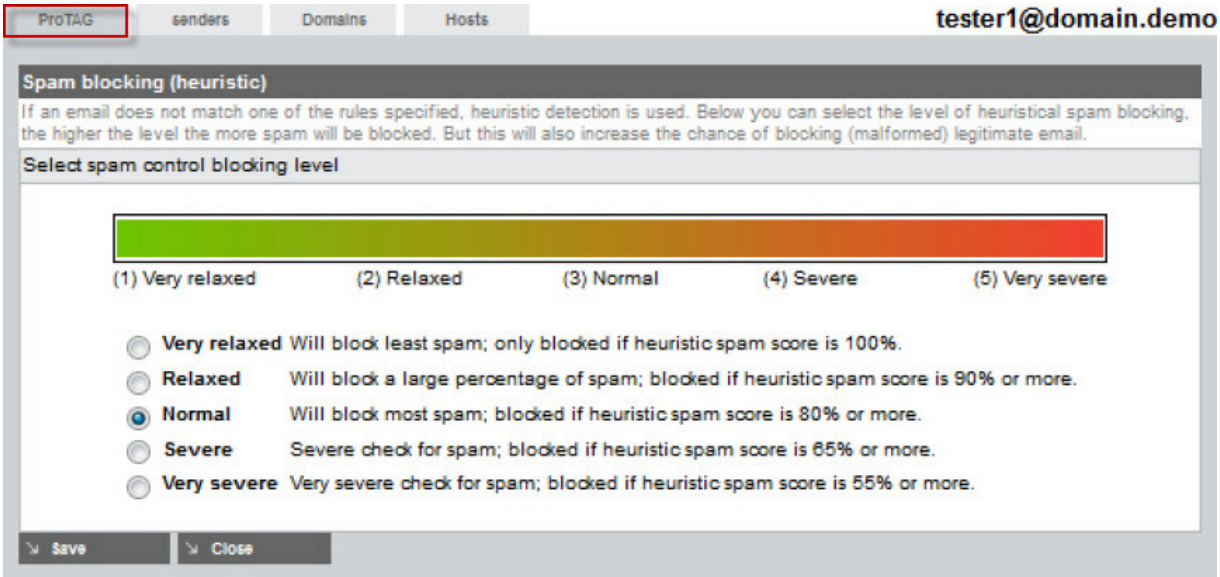
In the section of *Quarantine settings*, you can select the action you want to apply to infected Emails, spam Emails or filtered content.
The option *Type of quarantine release* gives you the opportunity to configure for each user how the infected Emails should be sent after the release from quarantine. The new settings will be activated only after a click on the **Save** button.

5.2. Adjusting the Spam Filter

The spam filter might be adjusted individually for each user. Therefore, select a User, go to the *Services* tab and click on **Advanced settings** for the filter you'd like to adjust.



On the page for the **Advanced Settings** are four tabs with different setting options. With a click on the *ProTAG* tab you can set the blocking level for the heuristic spam control, which is applied to your incoming Emails.

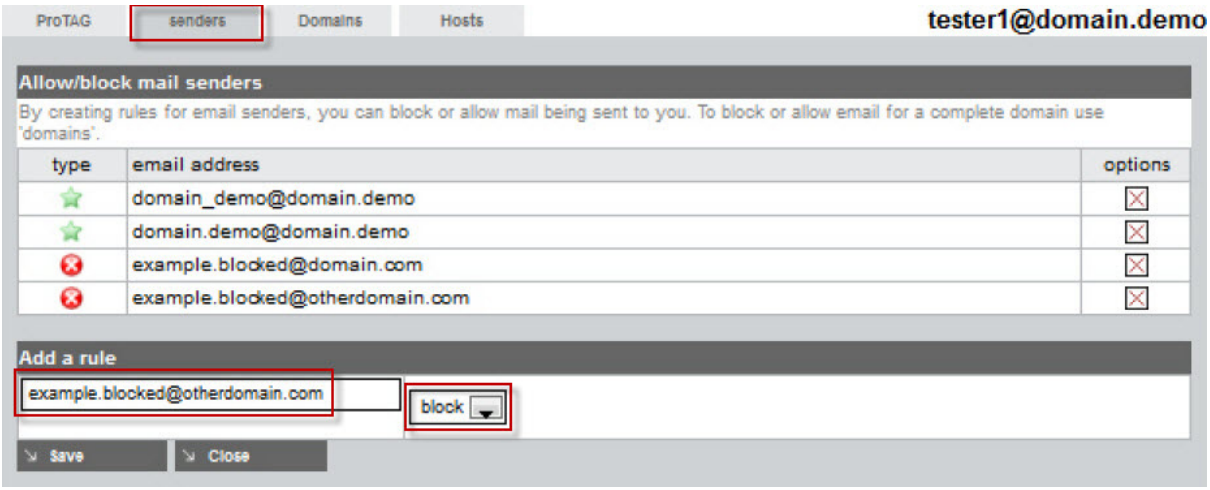

ProTAG
senders
Domains
Hosts
tester1@domain.demo
Spam blocking (heuristic)
If an email does not match one of the rules specified, heuristic detection is used. Below you can select the level of heuristical spam blocking, the higher the level the more spam will be blocked. But this will also increase the chance of blocking (malformed) legitimate email.
Select spam control blocking level
(1) Very relaxed
(2) Relaxed
(3) Normal
(4) Severe
(5) Very severe
Very relaxed Will block least spam; only blocked if heuristic spam score is 100%.
Relaxed Will block a large percentage of spam; blocked if heuristic spam score is 90% or more.
Normal Will block most spam; blocked if heuristic spam score is 80% or more.
Severe Severe check for spam; blocked if heuristic spam score is 65% or more.
Very severe Very severe check for spam; blocked if heuristic spam score is 55% or more.
Save
Close

If you adjust the spam filter on **Sever** or **Very sever**, it is possible that legitimate Emails are blocked by spam-like characteristics (False Positive). In this case a regular check of the spam quarantine is essential and must be performed on a regular basis with a scheduled daily spam report.

Furthermore, there is an option to release direct out of the report unwarranted Emails from the quarantine, then *whitelist* them and deliver them to your own mailbox.

Under the tab *senders*, you can create rules that allow you to block or permit Emails from certain senders. Therefore, insert the desired Email address of the sender in the field below *Add a rule*. Then set the type of rule to *block* or *allow*, and click **Save** to add the rule.

To delete a rule, click the **X** mark in the *options* column and click **OK** in the pop-up window.



Use the *Domains* and *Hosts* tabs to add rules for blocking or allowing certain domains and IP addresses.

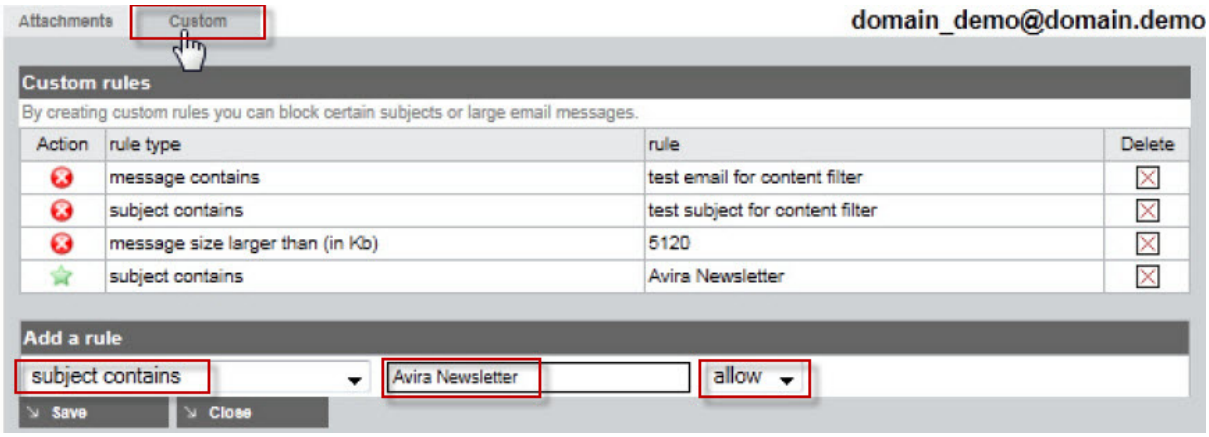
5.3. Adjusting the Content Filter

To configure the *Content Filter* select first the desired user, then go to the *Content* tab and click **Advanced settings** for the content filter. Below the tabs *Attachments* and *Custom* you can block the Email attachments for certain file types.

The *Attachments* tab includes three predefined options:

- block: block the corresponding file types.
- block if unsure: if you are not sure whether you want to allow this kind of attachment, we recommend that you block it.
- do not block: attachments accepted by default; you can block them if you want.

Below the *Custom* tab you have the possibility to create your own special rules. The Emails can be blocked based on specific topics or size.

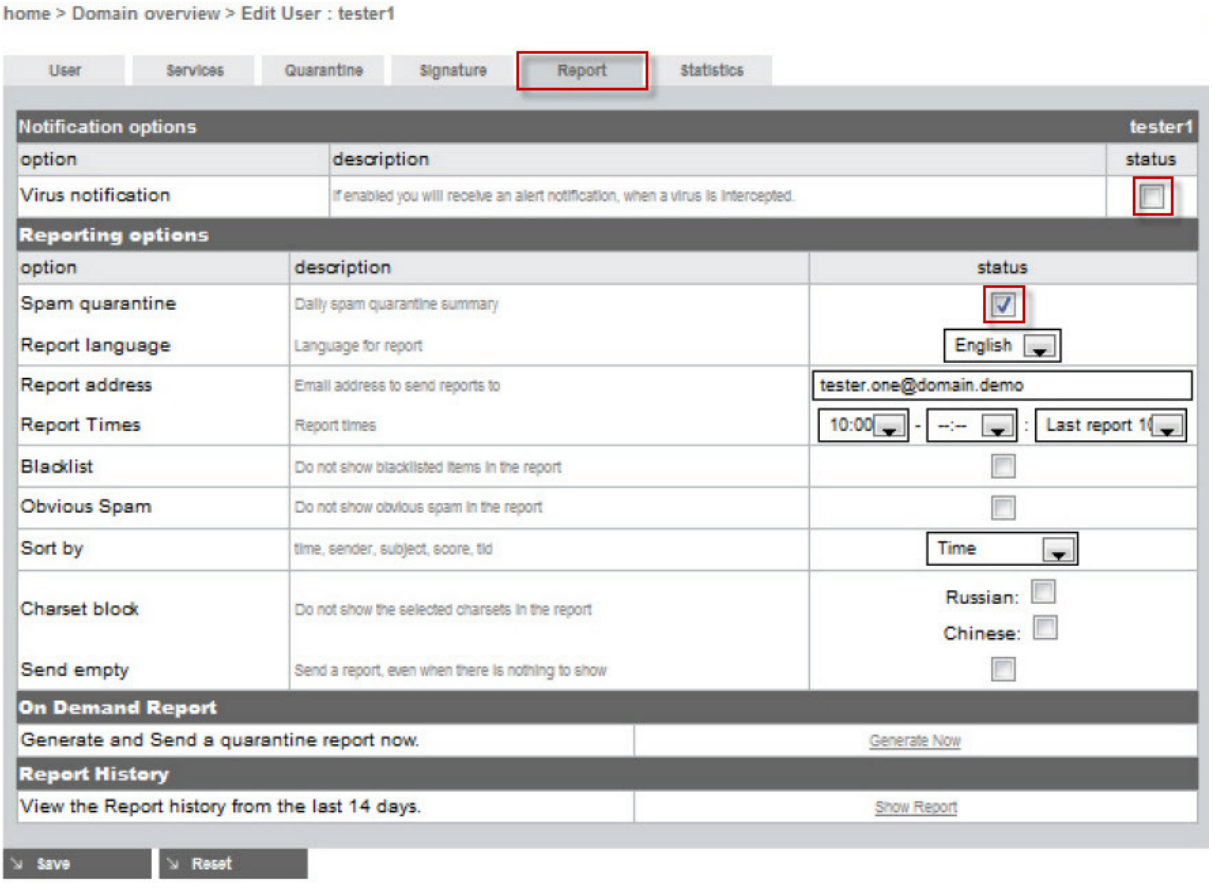


To delete a rule, click the **X** mark in the *Delete* column and click **OK** in the pop-up window.

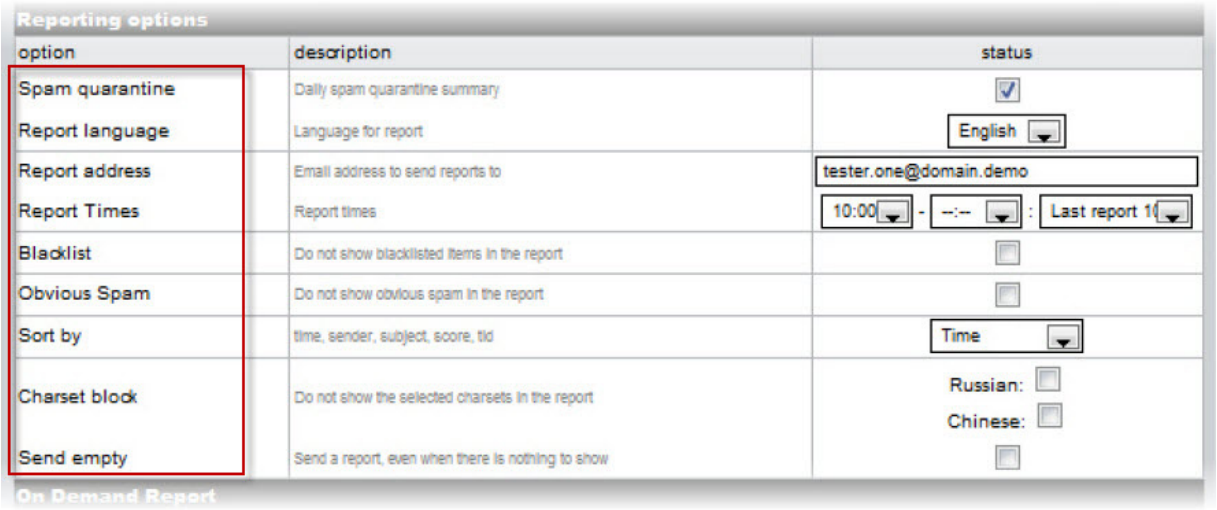
5.4. Setting up virus and spam notifications

To schedule a report, select a user and click the *Report* tab. There you can enable *Virus notification*, to receive a warning by Email, whenever a virus is intercepted.

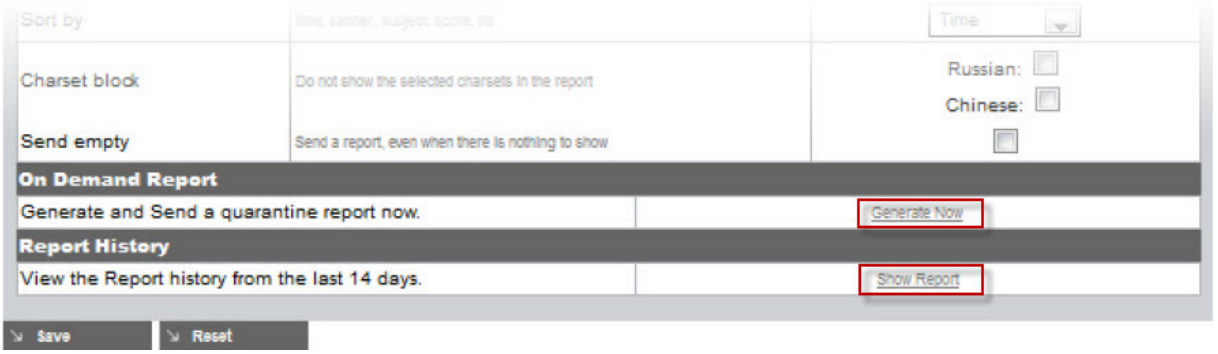
Enable also *Spam quarantine* if you want to receive a daily summary of intercepted spam.



Under the menu *Reporting options* you have the possibility to configure the Quarantine report as required. With a click on **Save** the new configuration will be active.



Click **Generate Now**, if you want to receive the quarantine summary per Email immediately. To view a report history of the last 14 days, click **Show Report**.

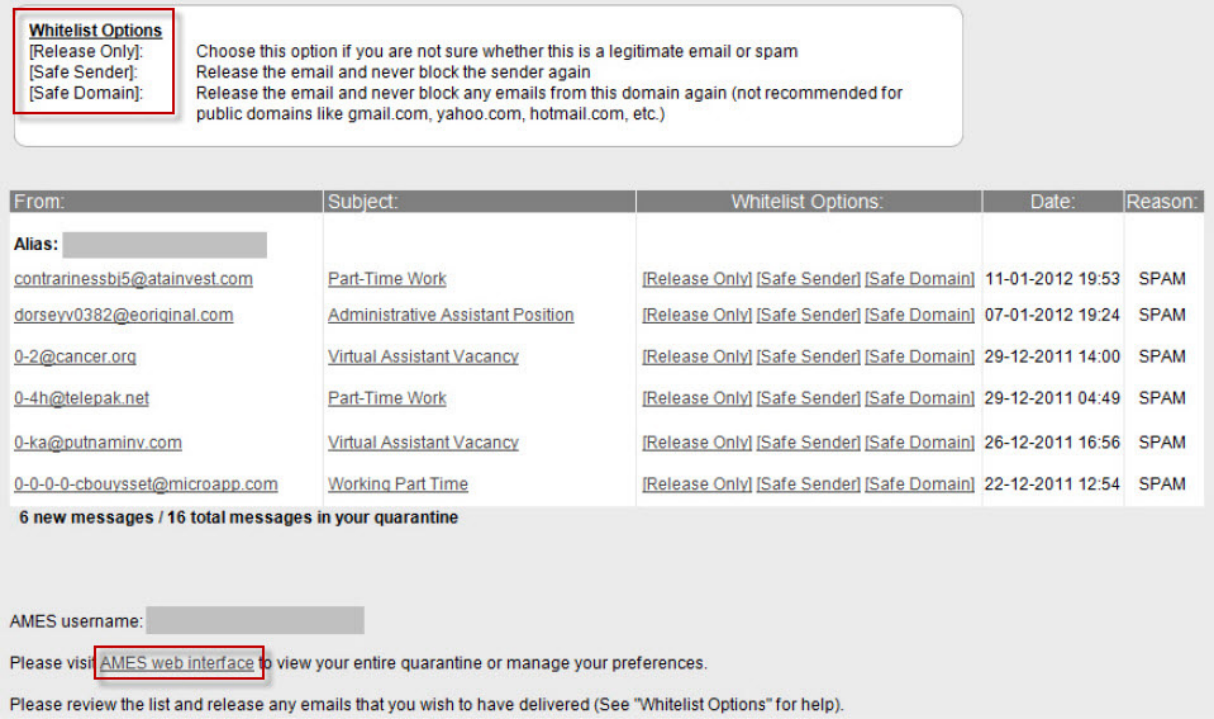


Note
We advise to let AMES generate a report on a daily basis, especially when you have just started using AMES or if you use severe filtering settings for spam.

As Avira Partner or AMES domain administrator, you can generate a quarantine report and send it to all users of a domain: Go to the *Domain overview* > *Services*, scroll down to the *Quarantine report* section and click **Send**.

5.5. Managing the quarantine via the Email account

If the daily summary report is enabled, the user will receive an everyday Email with a list of eventual new spam messages. The user can therefore manage his quarantine over his Email client by using the links in the *Whitelist Options*.



You can first check the details of the quarantined message, by clicking its subject in the *Subject* column of the Quarantine Summary.

If you identify an Email as safe, you can release the message from quarantine by clicking **Release this message**.

If you wish to view your entire quarantine or manage your preferences, you can click the link to the **AMES web interface**, which opens the login page to your AMES account.

Note
It is not recommended to use the Safe Domain option for public domains, such as gmail.com, yahoo.com, hotmail.com, etc.

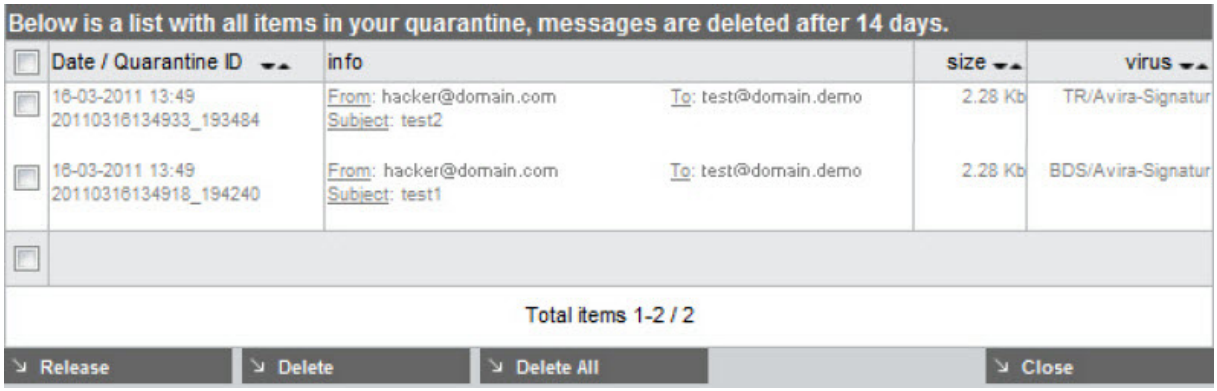
5.6. Managing the quarantine via the AMES account

To get to the quarantine, select a user and click the *Quarantine* tab. The AMES admin has the possibility to define the behavior of infected Emails. The Emails can be forwarded to the user without the infected attachments. The virus will be removed immediately from the Email and the Email will be delivered without attachment to the user.

AMES has three predefined types of quarantines, each with different filtering. Click on the name of a quarantine to check their content.

5.6.1 Virus quarantine

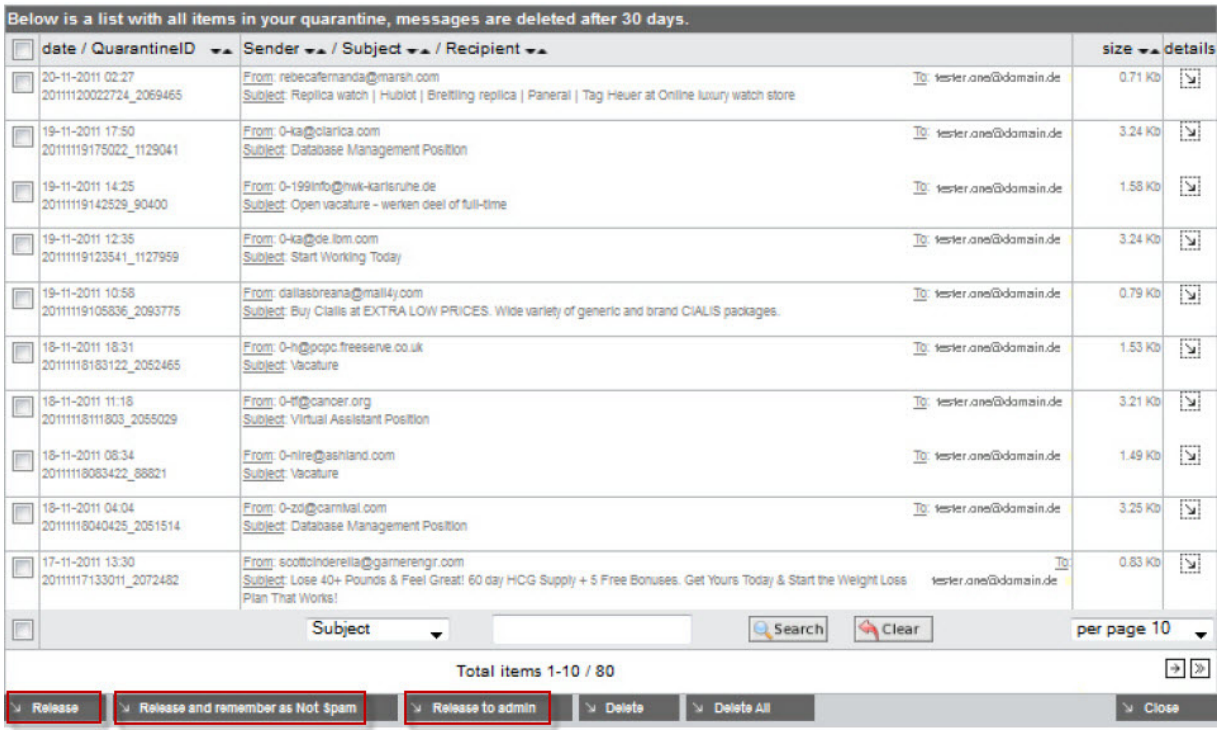
The **Virus quarantine** stores all Emails with virus signatures for 14 days, before they are automatically deleted. When you open the quarantine all Emails inside the quarantine can be viewed, manually deleted or released.



5.6.2 Spam quarantine

If your account is set to quarantine spam Emails for 30 days, the **Spam quarantine** stores all intercepted spam Emails. After expiration of the 30 days, the Emails are automatically deleted from the **Spam quarantine**.

Spam quarantine also includes a search feature to find easier certain Emails.



The release of Emails from the quarantine can be done in three different ways:

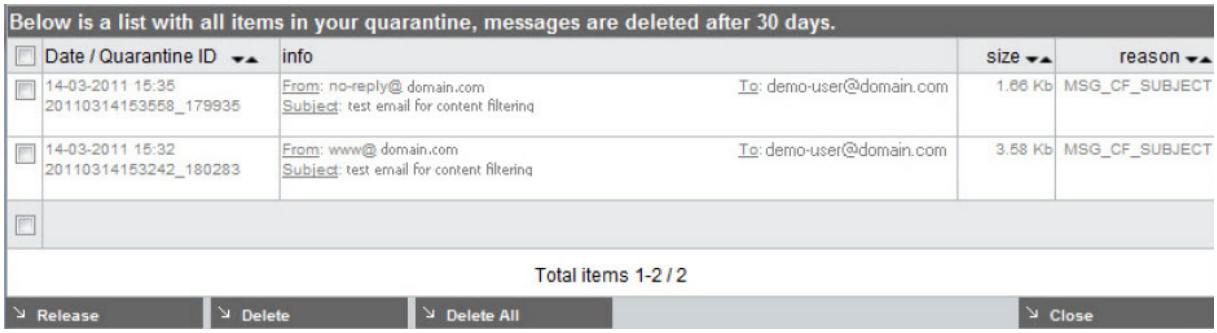
- **Release**
  With this button only the particular highlighted Email will be released

- **Release and remember as Not Spam**
  With this release the corresponding highlighted message will be released and all other messages from the same sender will no longer be treated as spam

- **Release to admin**
  The release of Emails with this option, sends all selected Emails to the account of the administrator for review

5.6.3 Content Filter quarantine

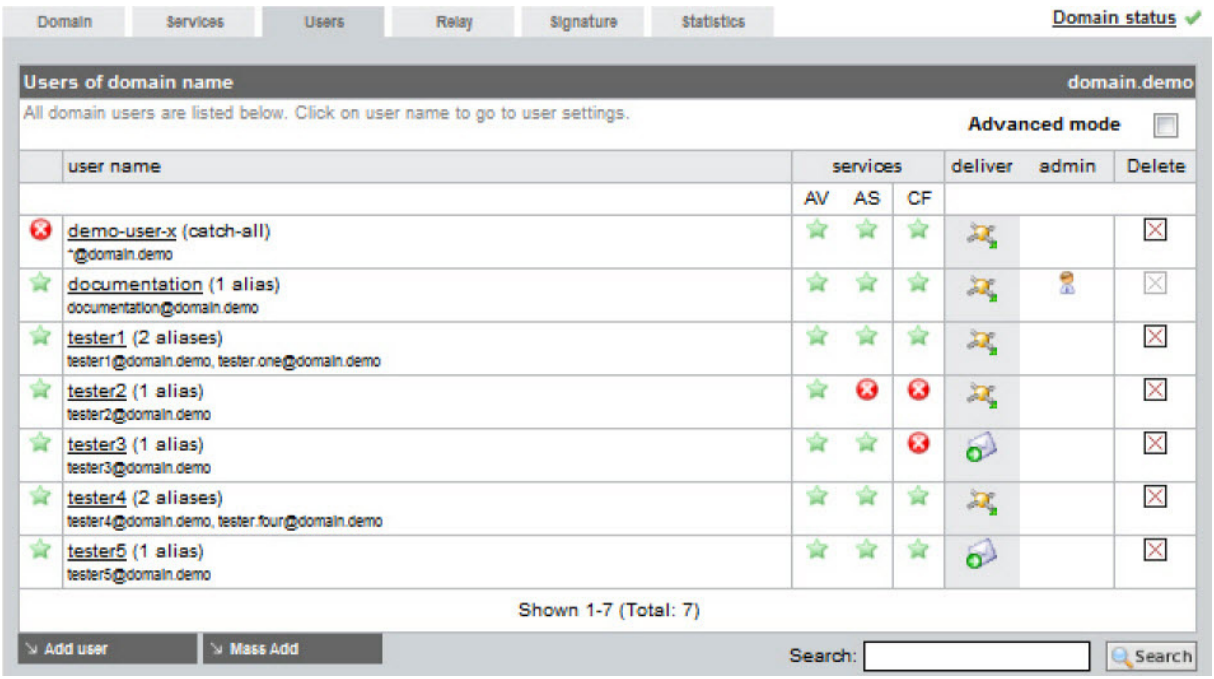
In the **Content Filter quarantine** you will find all blocked Emails, based on size, attachment or your own customized rules. They will be delete by default after 30 days.



6. User management

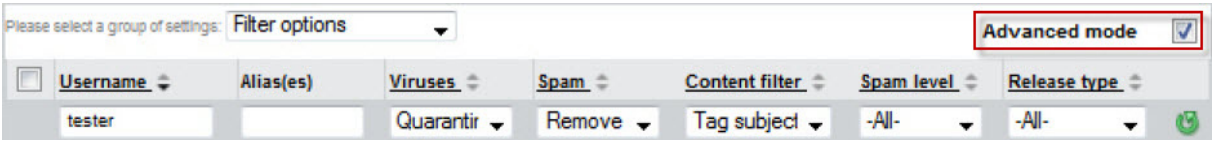
As AMES domain administrator, you can manage all the users of a domain in the *Domain overview*, on the *Users* tab.

The main view shows a list of users with the respective service status. You can access the settings of any respective user with a click on his name.



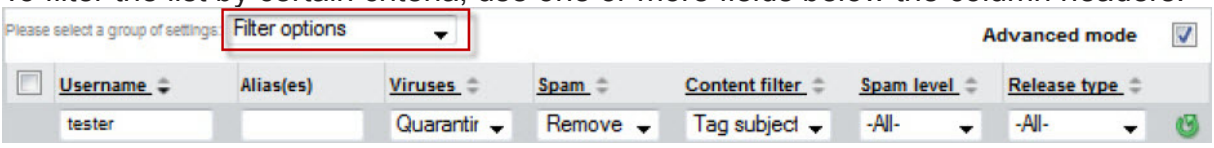
6.1. Advanced mode

If you enable the *Advanced mode* option, you can easily configure the services for single or multiple users in just three steps.



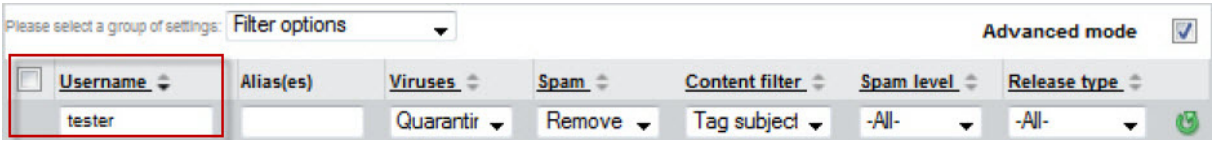
- **Select the group of settings**

To filter the list by certain criteria, use one or more fields below the column headers.

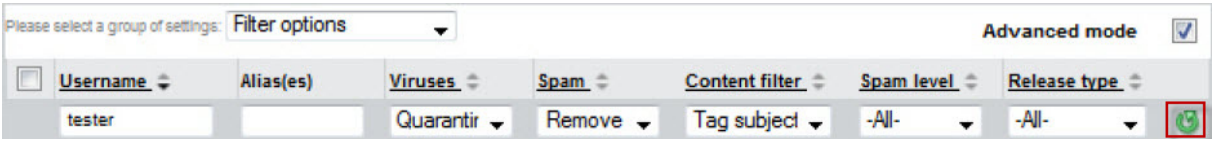


- **Select the users**

Click the checkboxes in the first column, to select the users. You can use the check-box in the table header, to select or deselect all users.



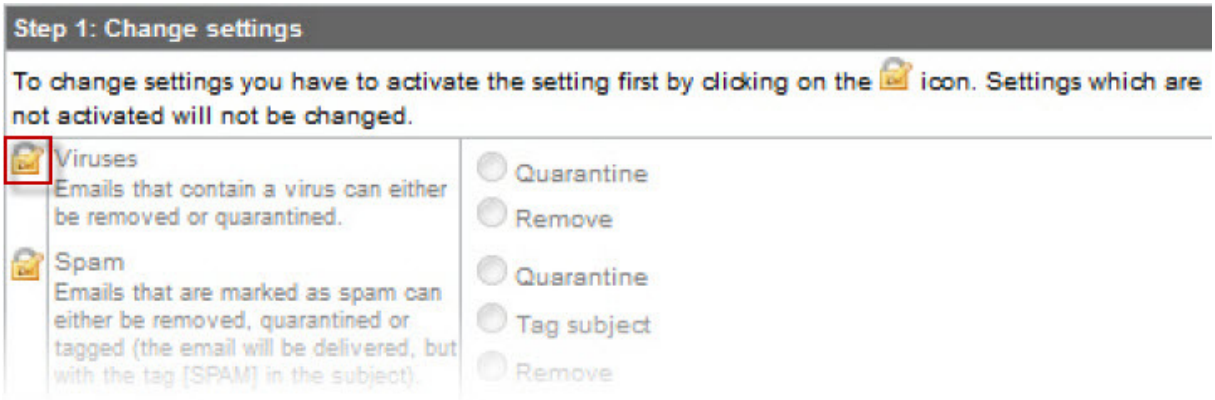
To clear all the filters and display the entire users list again, click the **Reset filters** button.



- **Change the user settings**

Click the **Edit selected** button, to start editing the services for the selected users. You can directly click **Edit all**, if the changes should apply to all users in the list.

Click the Edit icon in the first column of the settings sheet and select the option you want to activate for the selected users.


Step 1: Change settings
To change settings you have to activate the setting first by clicking on the icon. Settings which are not activated will not be changed.
Viruses
Emails that contain a virus can either be removed or quarantined.
Quarantine
Remove
Spam
Emails that are marked as spam can either be removed, quarantined or tagged (the email will be delivered, but with the tag [SPAM] in the subject).
Quarantine
Tag subject
Remove

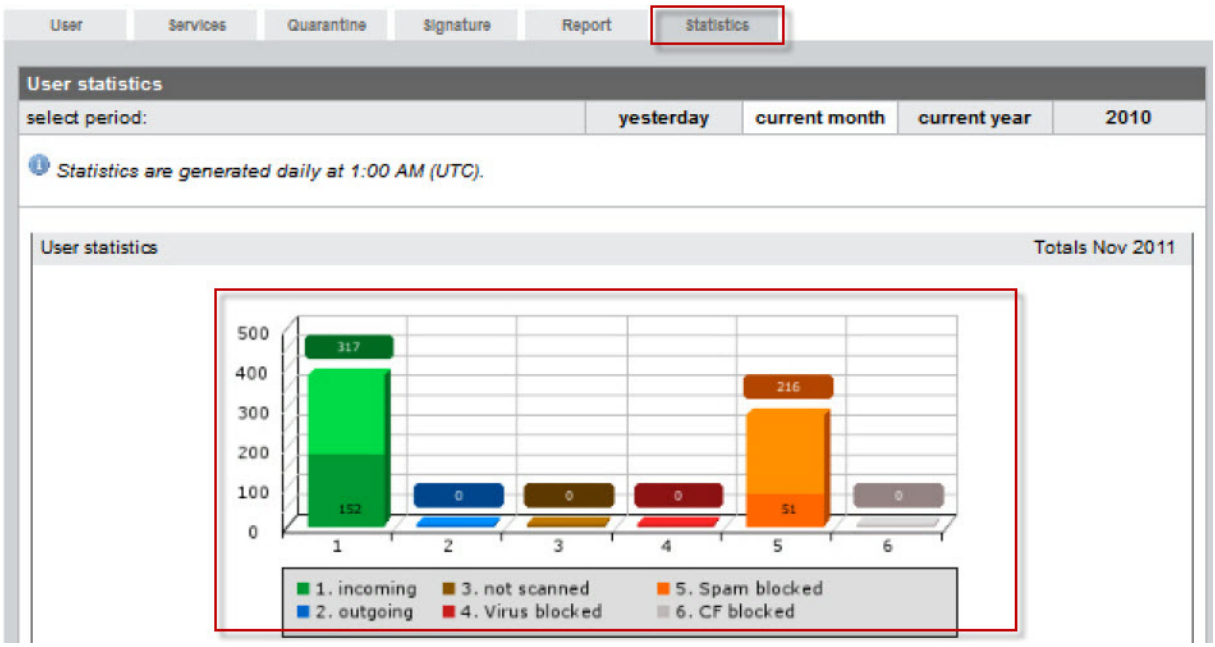
Once you have made the necessary changes click **Next** to review the changes. The changes you made will be updated in the *Users* view after clicking **Apply**, then **Close**.

7. Statistics

Below the *Statistics* tab all important information are displayed concerning the amount of Emails that Avira has handled for you.

If you are on the *domain* level, you can view all the data. At the *User* level, you can see only your own personal statistics.

The information about the processed Emails is divided into: *incoming, outgoing, not scanned, Virus blocked, Spam blocked* and *CF blocked*.



You can change the time range of the statistics, using the *select period* menu: yesterday, current month, last month, current year, or the previous year.

If you select for example, the current month, *day-by-day statistics* are also available for the selected user or domain.

Similarly, if you select a year, you can see *month-by-month statistics,* for a user or domain.

You can also check the report on the „Top 10“ viruses that have been intercepted by AMES in the selected period.

Further statistics display the „Top 25“ senders and „Top 25“ recipients of Emails during the selected period.

8. Support

- **Support service**

All necessary information on our comprehensive support service can be obtained from our website.

- **Contact**

Address
Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Germany

- **Internet**

You can find further information about us and our products at the following address:
http://www.avira.com

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira Operations GmbH & Co. KG.

Issued Q4-2012

Brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.

AVIRA

live free.™

© 2012 Avira Operations GmbH & Co. KG. All rights reserved.
Errors and omissions excepted.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile +49 7542-500 3000
www.avira.com